AN 1998-161979 JAPIO
TI USER AUTHENTICATION BY FINGERPRINT AT TIME OF LOG-IN TO SERVER AND CONVERTED PASSWORD
IN ISONO TAKAO; KATO TOMOYA
PA HITACHI LTD
PI ***JP 10161979*** A 19980619 Heisei
AI JP 1996-315924 (JP08315924 Heisei) 19961127
PRAI JP 1996-315924 19961127
SO PATENT ABSTRACTS OF JAPAN (CD-ROM), Unexamined Applications, Vol. 1998
IC ICM G06F015-00
AB PROBLEM TO BE SOLVED: To prevent illegal log-in even when a user ID and a password are stolen in the case of user authentication by the user ID and the password at a system where a client utilizes a server.
SOLUTION: A fingerprint recognizing device 30 is added to a client 20, three input requests of user ID, password and fingerprint are outputted at the time of user log-in, when the fingerprint relevant to the user ID is inputted, the inputted password is converted and a certificate request is outputted to a server 10 by the inputted user ID and the converted password. At the client 20, the algorithm for converting the password is programmed. The user ID and the password to be converted on the side of client 20 are previously registered in the server 10. This password registered in the server 10 is made different from the password to be inputted by the user, and made secret. The user is certified by the inputted user ID and the secret password registered in the server 10.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開平10－161979
(43)公開日　平成10年(1998)６月19日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｆ
			３３０Ｅ

審査請求　未請求　請求項の数１　ＯＬ　（全４頁）

(21)出願番号　特願平8－315924

(22)出願日　平成８年(1996)11月27日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　磯野　孝雄
神奈川県川崎市幸区鹿島田890番地の12
株式会社日立製作所情報システム事業部内
(72)発明者　加藤　友哉
愛知県名古屋市中区栄三丁目10番22号　日立中部ソフトウェア株式会社内
(74)代理人　弁理士　小川　勝男

(54)【発明の名称】　サーバへログイン時の指紋、及び変換したパスワードによるユーザ認証

(57)【要約】
【課題】サーバをクライアントが利用するシステムにおいて、ユーザＩＤとパスワードによるユーザ認証の際、ユーザＩＤとパスワードが盗まれた場合でも、不正ログインを防止できるようにする。
【解決手段】クライアントに指紋認識装置を付け、ユーザログイン時に、ユーザＩＤ、パスワード、指紋の３つの入力要求を出し、ユーザＩＤに該当する指紋が入力された場合、入力されたパスワードを変換し、入力されたユーザＩＤと変換されたパスワードでサーバへ認証要求を出す。クライアントではパスワードを変換するアルゴリズムを組み込んでおく。サーバにはあらかじめ、ユーザＩＤとクライアント側で変換されるパスワードを登録しておく。このサーバに登録されたパスワードは、ユーザが入力するものとは異なり、秘密にしておく。ユーザの認証は入力されたユーザＩＤとサーバに登録された秘密のパスワードで行う。

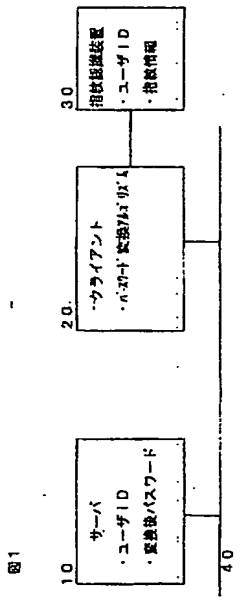


図1

1

【特許請求の範囲】

【請求項１】クライアントからユーザがサーバへログインするシステムにおいて、クライアントに指紋認識装置を接続しておき、ログイン時に、ユーザＩＤとパスワードにより、ユーザ認証を行う際、クライアント側で、ユーザがユーザＩＤ、パスワード入力後に、指紋入力要求を出し、ユーザＩＤに該当する指紋が入力されたか判定し、ユーザＩＤに該当する指紋が入力された場合、パスワードにアルゴリズムで変換をかけ、入力されたユーザＩＤと変換したパスワードでサーバに対し認証要求を出し、サーバはユーザ認証を行い、認証の可否をクライアントに通知し、ログイン完了または、ログイン拒否とし、ユーザＩＤに該当しない指紋が入力された場合、ログイン拒否とするユーザ認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、コンピュータシステムにおいて、クライアントからサーバにログインする際のユーザ認証方法に関する。

【０００２】

【従来の技術】サーバへユーザがログインする際、クライアントから入力された、ユーザＩＤとパスワードにより、サーバがユーザ認証を行う。指紋認証を個人識別に用いた技術は、その装置の使用可否の認証、例えばドアの開閉やパソコンの使用可否に利用されている。クライアントサーバシステムのユーザ認証に指紋認識を適用した場合、サーバ、クライアント両者に指紋にユーザ認証の仕組みを作り込む必要がある。

【０００３】本発明は、ユーザＩＤとパスワードによるユーザ認証と指紋によるユーザ認証を組み合わせ、クライアント側だけの変更で、より高度なセキュリティを実現するものである。

【０００４】

【発明が解決しようとする課題】従来の、サーバへのログイン時にクライアントから入力されたユーザＩＤとパスワードによるユーザ認証では、入力時に盗み見されて、ユーザＩＤとパスワードが盗まれ、不正ログインされる欠点があった。

【０００５】本発明の目的は、ユーザＩＤとパスワードが盗まれた場合でも、不正ログインを防止することにある。

【０００６】

【課題を解決するための手段】上記目的を解決するため、本発明ではクライアントに指紋認識装置を付け、ユーザログイン時に、ユーザＩＤ、パスワード、指紋の３つの入力要求を出し、ユーザＩＤに該当する指紋が入力された場合、入力されたパスワードを変換し、入力されたユーザＩＤと変換されたパスワードでサーバへ認証要求を出す。クライアントではパスワードを変換するアルゴリズムを組み込んでおく。サーバにはあらかじめ、ユーザＩＤとクライアント側で変換されるパスワードを登録しておく。このサーバに登録されたパスワードは、ユーザが入力するものとは異なり、秘密にしておく。ユーザの認証は入力されたユーザＩＤとサーバに登録された秘密のパスワードで行う。

2

【０００７】

【発明の実施の形態】本発明の一実施例について図面により詳細に説明する。

【０００８】図１は本発明を適用したシステムの一実施例のシステム構成図である。図１において、１０はサーバ、２０はクライアント、３０は指紋認識装置、４０はサーバ１０とクライアント２０を結ぶＬＡＮ等の通信回線である。本実施例ではクライアントは１台しか示されていないが、勿論、実際にはこれ以上のクライアントがサーバ１０と結ばれていることは云うまでもない。

【０００９】サーバ１０には、ユーザＩＤとパスワードが登録してあり、クライアント２０から送信されるユーザＩＤとパスワードで認証され、クライアント２０がサーバ１０の機能を利用することができる。指紋認識装置３０はユーザＩＤと指紋データのデータベースを持ち、ユーザＩＤと指紋の照合を行い、クライアント２０はパスワードを変換するアルゴリズムを有し、パスワード変換を行う。

【００１０】次に、本ユーザ認証の方法を図２のフローチャートに従い説明する。図２は、クライアント２０がサーバ１０へログインが完了するまでの流れを示したものである。クライアント２０がサーバ１０へログインを行うために、ユーザＩＤとパスワードを入力する（ステップ１００）。

【００１１】クライアント２０に指紋入力要求が表示され、ユーザは指紋認識装置に指紋を入力する（ステップ１１０）。指紋認識装置３０はユーザＩＤと入力された指紋が正しいか照合を行い、結果をクライアント２０へ通知する（ステップ１２０）。クライアント２０は指紋認識装置３０から通知された結果を判断し（ステップ１３０）、ＮＧの場合、ユーザＩＤ、パスワード入力画面にエラー表示する。ＯＫの場合、クライアント２０は入力されたパスワードを変換アルゴリズムに従い変換する（ステップ１４０）。クライアント２０は入力されたユーザＩＤと変換されたパスワードをサーバ１０へ送信する（ステップ１５０）。サーバ１０は受信したユーザＩＤとパスワードが、サーバ１０に登録されているユーザＩＤとパスワードと等しいか照合する（ステップ１６０）。照合結果を判断し（ステップ１７０）、結果がＮＧの場合クライアント２０にエラー通知を行う。結果がＯＫの場合、ログイン完了をクライアント２０へ通知する（ステップ１８０）。以上で、サーバ１０とクライアント２０のユーザ認証処理は完了し、クライアント２０はサーバ１０を利用することが可能となる。

【００１２】次に、ユーザＩＤとパスワードの関係を具

体例を用いて説明する。

【００１３】例えば、サーバ１０に登録されたユーザＩＤがｕｓｅｒ１、パスワードが１２３４５とした場合、クライアント２０でユーザが入力するユーザＩＤはｕｓｅｒ１、パスワードはＡＢＣＤＥとする。クライアント２０のパスワード変換アルゴリズムはＡＢＣＤＥを１２３４５に変換するものを作り込んでおく。この場合のユーザ認証の流れは、クライアント２０にユーザＩＤ　ｕｓｅｒ１、パスワードＡＢＣＤＥが入力される。指紋認識装置３０はユーザＩＤ　ｕｓｅｒ１に該当する指紋が入力されたか照合し、正しい場合クライアント２０はパスワードＡＢＣＤＥを１２３４５に変換し、サーバ１０へ照合を依頼する。ここでユーザ認証の完了となる。

【００１４】サーバにはユーザＩＤとパスワードによる認証しかなくても、クライアントに本発明を適用すれば、より高度なセキュリティを確保することが可能となる。

【００１５】

【発明の効果】以上説明したように、既存のクライアント＊

＊トがサーバを利用する製品にこの方法を適用すれば、正規ユーザが本発明を適用したクライアントからユーザＩＤ、パスワードを入力するところを不正ユーザが盗み見し、指紋認識装置のないクライアント製品（既存の製品）を用意して、サーバへログインを試みても、サーバでは、パスワードが異なるため、ログインを拒否する。

【００１６】このように、本発明の適用で、セキュリティを大幅に向上できる。

【図面の簡単な説明】

【図１】本発明の一実施例を示すシステム構成図である。

【図２】ユーザ認証の方法を示すフローチャートである。

【符号の説明】

１０　サーバ

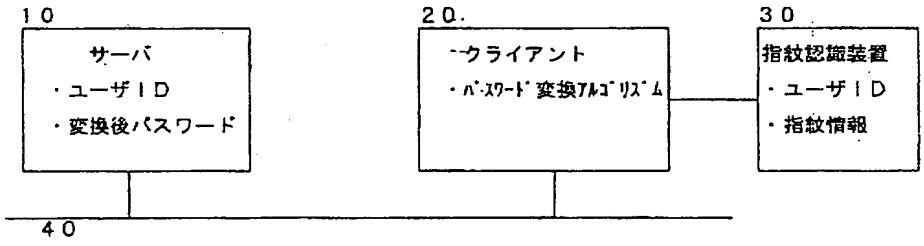
２０　クライアント

３０　指紋認識装置

４０　通信回線。

【図１】

図１



【図2】

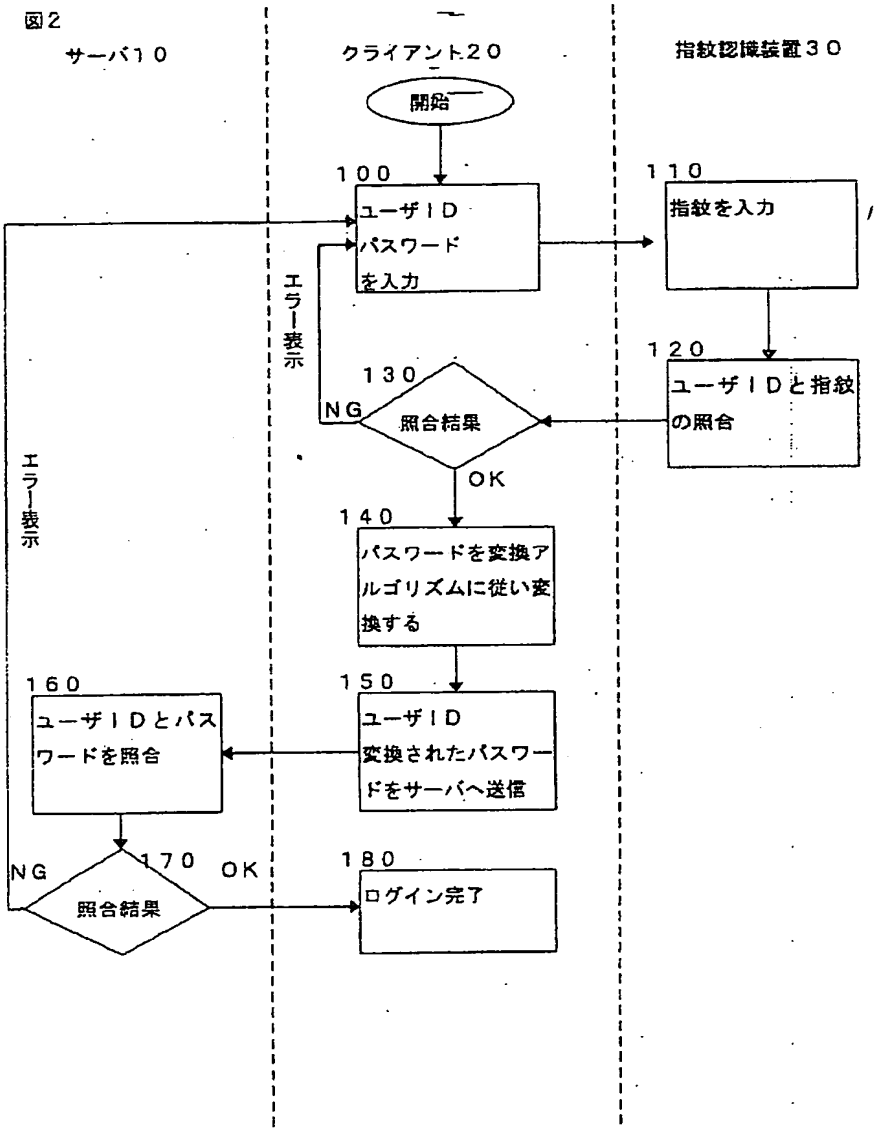


図2
サーバ10
クライアント20
指紋認識装置30
開始
100
ユーザID
パスワード
を入力
110
指紋を入力
120
ユーザIDと指紋
の照合
130
照合結果
NG
OK
エラー表示
エラー表示
140
パスワードを変換アルゴリズムに従い変換する
150
ユーザID
変換されたパスワードをサーバへ送信
160
ユーザIDとパスワードを照合
170
照合結果
NG
OK
180
ログイン完了